Available online at www.sciencedirect.com

ScienceDirect

Journal of Combinatorial Theory, Series A 113 (2006) 1677–1688

Journal of Combinatorial Theory Series A

www.elsevier.com/locate/jcta

A symmetric Roos bound for linear codes

Iwan M. Duursma [a], Ruud Pellikaan [b]

[a] *Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 W. Green Street, MC-382, Urbana, IL 61801-2975, USA*

[b] *Department of Mathematics and Computing Science, Eindhoven University of Technology, PO Box 513, 5600 MB Eindhoven, The Netherlands*

Received 30 September 2005

Available online 12 July 2006

Abstract

The van Lint–Wilson AB-method yields a short proof of the Roos bound for the minimum distance of a cyclic code. We use the AB-method to obtain a different bound for the weights of a linear code. In contrast to the Roos bound, the role of the codes A and B in our bound is symmetric. We use the bound to prove the actual minimum distance for a class of dual BCH codes of length $q^2 - 1$ over $\mathbb{F}_q$. We give cyclic codes $[63, 38, 16]$ and $[65, 40, 16]$ over $\mathbb{F}_8$ that are better than the known $[63, 38, 15]$ and $[65, 40, 15]$ codes.

Keywords: Roos bound; Minimum distance bound; Cyclic code; Dual BCH code

1. Introduction

Starting with the Hamming codes and the Golay codes in the late 1940's, cyclic codes have always played a central role in the theory of error-correcting codes. Reed–Muller codes, BCH codes and in particular Reed–Solomon codes have found widespread applications. Although some negative results are known indicating that cyclic codes are asymptotically bad, this remains an open problem. For moderate length, many optimal codes are cyclic. Binary cyclic codes are better than the Gilbert–Varshamov bound for lengths up to 1023. Rich mathematics is involved in the determination of the actual parameters of a cyclic code in terms of its defining set. The first result in this direction was obtained by Bose and Ray-Chaudhuri [1,2] and Hocquenghem [11]. Their result is known as the *BCH bound*. The bound was generalized first by Hartmann and Tzeng [10], and then, using important new ideas, by Roos [18,19]. In [13], van Lint and Wil-

E-mail addresses: duursma@math.uiuc.edu (I.M. Duursma), g.r.pellikaan@tue.nl (R. Pellikaan).

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2006.03.020

son present further techniques that are often useful when the actual minimum distance exceeds the *Roos bound*. They are known as the *AB-method* and the *Shifting method*. The various lower bounds for the minimum distance of a cyclic code are in general not sharp. And the efficient determination of the minimum distance of a cyclic code in general remains an open problem. In this paper we prove two bounds for the minimum distance of a general linear code, the iterated Roos bound (Theorem 8) and the symmetric Roos bound (Theorem 20). As an application, we give the actual parameters for a class of dual BCH codes (Theorem 24).

The following notation and terminology applies throughout. The finite field with q elements is denoted by $\mathbb{F}_q$. For a word $\mathbf{c} \in \mathbb{F}_q^n$, the Hamming weight of $\mathbf{c}$ is denoted by $\mathrm{wt}(\mathbf{c})$. The *support* of a word $\mathbf{c}$ is the set of nonzero positions of the word and is denoted by $\mathrm{supp}(\mathbf{c})$. The support of a subset D of $\mathbb{F}_q^n$ is defined as $\mathrm{supp}(D) = \{i \mid x_i \neq 0 \text{ for some } \mathbf{x} \in D\}$. The weight of D is the number of elements of $\mathrm{supp}(D)$ and is denoted by $\mathrm{wt}(D)$.

A q-ary code C is a linear subspace of $\mathbb{F}_q^n$. For a linear code C, let $n(C)$, $k(C)$ and $d(C)$ denote its length, dimension and minimum distance, respectively. The rth generalized Hamming weight of C is defined by $d_r(C) = \min\{\mathrm{wt}(D) \mid D \text{ linear subspace of } C,\ k(D) = r\}$. Define the *genus* or the *Singleton defect* of C as $g(C) = n(C) + 1 - k(C) - d(C)$. The genus is a nonnegative integer by the Singleton bound.

For two vectors $\mathbf{a}$ and $\mathbf{b}$ of the same length n, let $\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + \cdots + a_n b_n$ be the inner product, and let $\mathbf{a} * \mathbf{b} = (a_1 b_1, \ldots, a_n b_n)$ be the componentwise product. For two subsets A and B of $\mathbb{F}_q^n$, let $A * B, = \{\mathbf{a} * \mathbf{b} \mid \mathbf{a} \in A,\ \mathbf{b} \in B\}$. We say that A and B are orthogonal when $\mathbf{a} \cdot \mathbf{b} = 0$ for all $\mathbf{a} \in A$ and all $\mathbf{b} \in B$, we denote this by $A \perp B$. The dual $A^\perp$ of a subspace A is by definition $A^\perp = \{\mathbf{c} \in \mathbb{F}_q^n \mid \mathbf{c} \cdot \mathbf{a} = 0 \text{ for all } \mathbf{a} \in A\}$.

A code A is called *degenerate* if there is a position such that all code words in A are zero at that position, or equivalently $d(A^\perp) = 1$. For a subset A of $\mathbb{F}_q^n$, let $\langle A \rangle$ be the subspace generated by A. For a code A of length n and a subset $I \subset \{1, \ldots, n\}$, the subcode $A(I) = \{\mathbf{a} \mid a_i = 0 \text{ for all } i \in I\}$.

2. Two bounds for cyclic codes

Let $\mathbb{F}_q$ be a finite field of order q and for n with $(n, q) = 1$, let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$ containing the nth roots of unity. Let $\alpha \in \mathbb{F}_{q^m}$ be a primitive nth root of unity. Let $\alpha(i) = (1, \alpha^i, \alpha^{2i}, \ldots, \alpha^{(n-1)i})$. The $\mathbb{F}_{q^m}$ linear cyclic code with *generating set* $\{i_1, \ldots, i_s\}$ is by definition $C = \langle \alpha(i_1), \alpha(i_2), \ldots, \alpha(i_s) \rangle$, and the $\mathbb{F}_q$ linear cyclic code with *defining set* $\{i_1, \ldots, i_s\}$ is by definition the space of all words in $\mathbb{F}_q^n$ that are orthogonal to C. We formulate a special case of the Roos bound for cyclic codes.

Theorem 1 *(Roos bound for cyclic codes [18]). Let the cyclic codes A and B be defined as follows, for $i_1 < i_2 < \cdots < i_{s+1}$,*

$$A = \langle \alpha(i_1), \alpha(i_2), \ldots, \alpha(i_{s+1}) \rangle,$$
$$B = \langle \alpha(1), \alpha(2), \ldots, \alpha(\delta - 1) \rangle.$$

Let $i_{s+1} - i_1 - s < \delta - 1$. Then, a code C with $C \perp (A * B)$ has minimum distance $d(C) \geqslant \delta + s$.

For cyclic codes A, B and C it is easy to verify if $C \perp (A * B)$ given the defining set of C.

Lemma 2. *If A and B are the cyclic codes with generating set U and V, respectively, then $C \perp (A * B)$ if and only if the defining set for C contains $U + V = \{u + v \mid u \in U,\ v \in V\}$.*

The following symmetric version of the Roos bound rules out certain weights in a code and in general does not give a lower bound for the minimum distance. This is characteristic for the AB-method that is used for its proof.

Theorem 3 *(Symmetric Roos bound for cyclic codes). For* $i_1 < i_2 < \cdots < i_{s+1}$, *and* $j_1 < j_2 < \cdots < j_{t+1}$, *let*

$$A = \langle \alpha(i_1), \alpha(i_2), \ldots, \alpha(i_{s+1}) \rangle,$$
$$B = \langle \alpha(j_1), \alpha(j_2), \ldots, \alpha(j_{t+1}) \rangle.$$

Let $i_{s+1} - i_1 - s < t + 1$ *and* $j_{t+1} - j_1 - t < s + 1$. *Then, a word* $\mathbf{c}$ *with* $\mathbf{c} \perp A * B$ *has weight* $\mathrm{wt}(\mathbf{c}) \leqslant (i_{s+1} - i_1 - s) + (j_{t+1} - j_1 - t)$, *or* $\mathrm{wt}(\mathbf{c}) \geqslant s + t + 2$.

Proof. Combine Theorem 5 and Corollary 1 in [13]. Theorem 20 in Section 5 gives a generalization to linear codes. □

3. Bounds for linear codes

In [19], Roos derives the *Roos bound for cyclic codes* [19, Theorem 2] from a more general theorem [19, Theorem 1].

Theorem 4 *(Roos bound for linear codes [19, Theorem 1]). Let A, B and C be linear codes such that*

(0) $d(A^\perp) > 1$,
(1) $C \perp (A * B)$,
(2) $g(A) \leqslant d(B^\perp) - 2$.

Then $d(C) \geqslant d(B^\perp) + k(A) - 1$.

Proof. The proof in [19] applies after matching our notation with their notation. The formulation in [19] is in terms of a generating matrix $X = G_A$ for A and a generating matrix $A = G_B$ for B. And the bound is proven under the condition that every $m \times (m + d(B^\perp) - 2)$ submatrix of the $m \times n$ matrix X is of full rank. Clearly, this is equivalent to saying that X has no words with support on $n - (m + d(B^\perp) - 2)$ positions, or $d(A) > n - k(A) - d(B^\perp) + 2$. Finally, for genus $g(A) = n + 1 - k(A) - d(A)$, this can be written as $d(B^\perp) - 1 > g(A)$. □

The theorem is equivalent to the following proposition.

Proposition 5. [16] *Let A, B and C be linear codes of length n such that, for positive integers a and b*

(0) $d(A^\perp) > 1$,
(1) $C \perp (A * B)$,
(2) $k(A) > a$,

(3) $d(B^{\perp}) > b$,
(4) $d(A) > n - (a + b)$.

Then $d(C) > a + b$.

Note that conditions (2)–(4) imply that

$$k(A) + d(A) + d\big(B^{\perp}\big) > n + 2,$$

which is equivalent to

$$g(A) < d\big(B^{\perp}\big) - 1.$$

On the other hand, for $g(A) \leqslant d(B^{\perp}) - 2$, conditions (2)–(4) hold with $a = k(A) - 1$ and $b = d(B^{\perp}) - 1$. Thus Theorem 4 and Proposition 5 are equivalent. The proposition reveals the relation between the Roos bound and error-correcting algorithms. A pair of codes $A, B \subset \mathbb{F}_q^n$ is called *t-error-locating* for the code C if

(1) $C \perp (A * B)$,
(2) $k(A) > t$,
(3) $d(B^{\perp}) > t$.

If moreover the pair A, B satisfies

(4) $d(A) \geqslant n - d(C)$,

then the pair is called *t-error-correcting* for the code C [12,14,15]. The existence of error-correcting pairs has been shown for algebraic geometry codes and many binary cyclic codes [5,7–9,16,17,20,21]. If the conditions (1)–(4) hold in Proposition 5 with $a = b = t$, then the pair (A, B) is a t-error-correcting pair for C and t errors can be corrected efficiently. The decoding up to half the Roos bound or the Hartmann–Tzeng bound is still an open problem.

Proposition 5 has the following generalization.

Theorem 6. *Let A, B and C be linear codes of length n such that, for nonnegative integers a, b, r with $r \leqslant a$,*

(0) $d(A^{\perp}) > 1$,
(1) $C \perp (A * B)$,
(2) $k(A) > a$,
(3) $d(B^{\perp}) > b$,
(4) $d_r(A) \geqslant n - (a + b - r)$.

Then $d(C) \geqslant a + b + 2 - r$.

Proof. The proof is similar to the one in [16] for $r = 1$. Note that (1) implies that $C * A$ is contained in $B^{\perp}$. Let $\mathbf{c}$ be a nonzero code word of C of minimal weight $d(C)$.

First, assume $\mathrm{wt}(\mathbf{c}) \leqslant b$. With (0), we obtain a nonzero word $\mathbf{a} \in A$ with $a_i \neq 0$ and i in the support of $\mathbf{c}$. Then $\mathbf{c} * \mathbf{a}$ is a nonzero word in $B^{\perp}$ of weight $\mathrm{wt}(\mathbf{c} * \mathbf{a}) \leqslant b$. A contradiction with (3). Thus $\mathrm{wt}(\mathbf{c}) > b$.

Next, assume $b < \mathrm{wt}(\mathbf{c}) \leqslant a+b+1-r$. Let I^- be a subset of the support of $\mathbf{c}$ consisting of b elements, and I^+ an index set of $a+b+1-r$ elements which contains $\mathrm{supp}(\mathbf{c})$. Let $\mathbf{a} \in A$ such that $a_i = 0$ for all $i \in I^+ \setminus I^-$. Then the vector $\mathbf{c} * \mathbf{a}$ is an element of $B^\perp$ and has support in I^-. Furthermore $|I^-| = b < d(B^\perp)$. Hence $\mathbf{c} * \mathbf{a} = 0$ by (3), so $a_i = 0$ for all $i \in I^+$. Therefore $A(I^+) = A(I^+ \setminus I^-)$. Now $I^+ \setminus I^-$ consists of $a+1-r$ elements, and $k(A) \geqslant a+1$ by (2). Hence $A(I^+ \setminus I^-)$ is a subspace of A and its dimension is at least r. Therefore $\mathrm{wt}(A(I^+ \setminus I^-)) \geqslant n-(a+b-r)$ by (4). On the other hand, $\mathrm{wt}(A(I^+)) \leqslant n - |I^+| = n-(a+b+1-r)$. This is a contradiction, since $A(I^+) = A(I^+ \setminus I^-)$. Therefore $d(C) \geqslant a+b+2-r$. □

Because of the weaker condition in (4), Theorem 6 applies in some cases where Proposition 5 does not.

Example 7. Let C be the binary Reed–Muller code $RM(2,5)$ with parameters $[32, 16, 8]$. And let $A = B$ be the binary Reed–Muller code $RM(1,5)$ with parameters $[32, 6, 16]$. Then $d(B^\perp) = 4$ and $d_3(A) = 28$ so that the conditions hold with $a = 5, b = 3$ and $r = 3$. This gives $d(C) \geqslant 7$, which improves to $d(C) \geqslant 8$ with the observation that all words in C are of even weight.

4. The iterated Roos-bound

Theorem 8. *Let $A_1, \ldots, A_m, B_1$ and C be $\mathbb{F}$-linear codes of length n such that, for all $i = 1, \ldots, m$,*

(0) $d(A_i^\perp) > 1$,
(1) $C \perp (A_m * \cdots * A_1 * B_1)$,
(2) $k(A_i) > a_i$,
(3) $d(B_1^\perp) > b_1$,
(4) $d(A_i) > n - (a_i + \cdots + a_1 + b_1)$.

Then $d(C) > a_m + \cdots + a_1 + b_1$.

Proof. The proof is by induction on m. For $m = 1$, we can use Proposition 5 with $A = A_1$ and $B = B_1$. For $i = 1, \ldots, m$, let $B_{i+1} = \langle A_i * B_i \rangle$ and let $C_{i+1} = B_{i+1}^\perp$. So that $C_{i+1} \perp A_i * \cdots * A_1 * B_1$. Suppose that, by the induction hypothesis for $i = m-1$, $d(C_m) > a_{m-1} + \cdots + a_1 + b_1$. Then Proposition 5 with $A = A_m$, $B = B_m$ and $C = C_{m+1}$ yields $d(C) > a_m + (a_{m-1} + \cdots + a_1 + b)$. □

For cyclic codes, we formulate the conditions in terms of the generating sets $U_1, \ldots, U_m, V_1$ for the codes $A_1, \ldots, A_m, B_1$, respectively. For a code A with generating set U we use that $k(A) = |U|$ and $d(A) \geqslant n - (|\bar{U}| - 1)$, where $\bar{U}$ is a set of consecutive integers that contains U.

Corollary 9. *Let $U_1, \ldots, U_m, V_1$ be nonempty subsets of $\mathbb{Z}_n$ and let $V_{i+1} = U_i + V_i$. Let d_1 be the minimum distance of the cyclic code over $\mathbb{F}$ with V_1 as defining set. If $|\bar{U}_i| \leqslant |U_i| + \cdots + |U_1| + d_1 - i - 1$ for all $i = 1, \ldots, m$, then the minimum distance of the cyclic code with defining set V_{m+1} is at least $|U_m| + \cdots + |U_1| + d_1 - m$.*

Remark 10. In case $m = 1$ we get the original Roos bound [13,18,19]. The special case $m = 2$ is still more general than Theorem 2 of [5]. In all cases, the minimum distance bound obtained with

the theorem is that of the Roos bound applied to $A = A_m$, $B = B_m$. The purpose of the theorem is therefore not to obtain better bounds than the Roos bound, but rather to facilitate the choice of sets A and B. We illustrate this for a class of codes.

Definition 11. Let q, m and s be nonnegative integers such that q is a power of a prime and $0 \leqslant s < q$. Let $n = q^m - 1$. Let $U(q, m, s)$ be the subset of $\mathbb{Z}_n$ defined by

$$U(q, m, s) = \{i_0 + i_1 q + \cdots + i_{m-1} q^{m-1} \mid 0 \leqslant i_j \leqslant s \text{ for } j = 0, \ldots, m-1\}.$$

Let $C(q, m, s)$ be the cyclic code of length n over $\mathbb{F}_q$ with $U(q, m, s)$ as defining set. The set $U(q, m, s)$ is invariant under multiplication by q and thus is a complete defining set.

Proposition 12. *The dual code $C(q, m, s)^\perp$ is the BCH code with a defining set $J = \{1, \ldots, (q-1-s)q^{m-1} - 1\}$ and parameters $n = q^m - 1$, $k = (s+1)^m$, and $d = (q-1-s)(q^m-1)/(q-1)$.*

Proof. The code $C(q, m, s)$ has complete defining set

$$U = U(q, m, s) = \{0 \leqslant i < n\colon\ 0 \leqslant i_j \leqslant s \text{ for } j = 0, \ldots, m-1\}.$$

It follows that the dual code has complete defining set

$$\begin{aligned} V &= \{0 < i < n\colon\ n - i \notin U\} \\ &= \{0 < i < n\colon\ i_j < q - 1 - s \text{ for some } j = 0, \ldots, m-1\}. \end{aligned}$$

The smallest i not in V is $i = (q-1-s)(q^m-1)/(q-1)$. Thus $J \subset V$. On the other hand, for every $i \in V$ there exists an $i' \in \{q^k i\colon\ k = 0, \ldots, m-1\}$ with $i'_{m-1} < (q-1-s)$. And thus $i' < (q-1-s)q^{m-1}$ and $i' \in J$. We have shown that J and V define the same code. The BCH bound for V gives $d \geqslant (q-1-s)(q^m-1)/(q-1)$. To show that this is the actual distance we need to show that there exist words with $s(q^m-1)/(q-1)$ zeros. Since U is a generating set, we can find words with zeros on any s distinct cosets of the $(q^m-1)/(q-1)$th roots of unity. □

Example 13. Let $V_1 = \{0, 1, \ldots, s\}$ and let $U_j = \{0, q^j, \ldots, sq^j\}$ for $j = 1, \ldots, m-1$. Define by induction $V_{j+1} = U_j + V_j$ for $j = 1, \ldots, m-1$. Then $V_j = U(q, j, s)$ and $\bar{U}_j = U_j$ for all j. So $|\bar{U}_j| = |U_j| = s + 1$ and $d_1 = s + 2$ and all the conditions of Corollary 9 are satisfied. Hence the minimum distance of $C(q, m, s)$ is at least $(m-1)s + (s+2) = ms + 2$.

The bound is sharp for $m = 2$, $n = q^2 - 1$ and $q \geqslant 2s + 1$. In that case, words with support among the $(q+1)$-roots of unity have a defining set that reduces modulo $q+1$ to the defining set

$$\{-s, -s+1, \ldots, -1, 0, 1, \ldots, s-1, s\}$$

which gives an MDS subcode of type $[q+1, q-2s, 2s+2]$. Hence the minimum distance of $C(q, 2, s)$ is equal to $2s + 2$ if $q \geqslant 2s + 1$.

Lemma 14. *Let $C = C(q, m, s)$ be the cyclic code of the previous example. For $0 \leqslant a \leqslant s$,*

$$(a+1)s \geqslant a(q+a-1) \quad \Rightarrow \quad d(C) \geqslant ms + 2 + a(s-a)(m-1).$$

Table 1
Codes of length 63 ($q = 8, m = 2$) and length 80 ($q = 9, m = 2$)

	$q = 8, m = 2$				$q = 9, m = 2$			
	C		$C^\perp = BCH$		C		$C^\perp = BCH$	
	dim	dist	dim	dist	dim	dist	dim	dist
$s = 0$	62	2	1	63	79	2	1	80
1	59	4	4	54	76	4	4	70
2	54	6	9	45	71	6	9	60
3	47	8	16	36	64	8	16	50
4	38	16	25	27	55	10	25	40
5	27	24	36	18	44	20	36	30
6	14	32	49	9	31	30	49	20
7					16	40	64	10

Proof. Let $V_1 = \{0, 1, \ldots, s-a\} + \{0, q, \ldots, aq\}$, and let $U_j = q^j V_1$, for $j = 1, \ldots, m-1$. Then $U(q, m, s) = U_{m-1} + \cdots + U_1 + V_1$. By the HT bound the code with defining set V_1 has minimum distance $d_1 \geqslant s + 2$. Also, for $j = 1, \ldots, m-1$,

$$|U_j| = (s - a + 1)(a + 1) \quad \text{and} \quad |\bar{U}_j| = aq + s - a + 1.$$

For the application of Corollary 9 the condition on $|\bar{U}_j|$ is strongest for $j = 1$,

$$\begin{aligned} &|\bar{U}_1| \leqslant |U_1| + d_1 - 2 \\ &\quad \Leftrightarrow \quad aq + s - a + 1 \leqslant (s - a + 1)(a + 1) + s \\ &\quad \Leftrightarrow \quad aq - a + a^2 \leqslant (a + 1)s. \end{aligned}$$

If the condition holds, then

$$\begin{aligned} d(C) &\geqslant |U_{m-1}| + \cdots + |U_1| + d_1 - (m - 1) \\ &= (m - 1)(s - a + 1)(a + 1) + s + 2 - (m - 1) \\ &= ms + 2 + a(s - a)(m - 1). \qquad \square \end{aligned}$$

Table 1 gives the actual parameters for codes $C(q, m, s)$ with $m = 2$ for $q = 8$ or $q = 9$. The values for the minimum distance $d(C)$ are obtained with Theorem 24.

5. The symmetric Roos bound

The following theorem is the main tool in the AB-method, due to van Lint and Wilson [13], for proving the minimum distance of cyclic codes.

Theorem 15. [13] *Let* $\mathbf{c} \perp A * B$. *Then*

$$\mathrm{wt}(\mathbf{c}) \geqslant k(\mathbf{c} * A) + k(\mathbf{c} * B).$$

Proof. We recall the short argument that is used in the original proof. Let I be the support of $\mathbf{c}$ and let π_I be the projection map onto I. Let $A' = \pi_I(\mathbf{c} * A)$ and $B' = \pi_I(B) \sim \pi_I(c * B)$. Then A' and B' are mutually orthogonal codes of length $\mathrm{wt}(\mathbf{c})$, such that $k(A') = k(\mathbf{c} * A)$ and $k(B') = k(\mathbf{c} * B)$. The sum of the dimensions of orthogonal spaces is at most the dimension of the ambient space. $\square$

Lemma 16. *Let $k = k(A)$, $l = k(\mathbf{c} * A)$ and $r = k - l$. If $r \geqslant 1$, then*

$$d_r(A) \leqslant n - \mathrm{wt}(\mathbf{c}).$$

Proof. Let $\mathbf{a}_1, \ldots, \mathbf{a}_k$ be a basis of A. If $l < k$, then after a permutation of this basis we may assume that $\mathbf{c} * \mathbf{a}_1, \ldots, \mathbf{c} * \mathbf{a}_l$ is a basis of $\mathbf{c} * A$. So $\mathbf{c} * \mathbf{a}_j$ is a linear combination of the $\mathbf{c} * \mathbf{a}_1$, $\ldots, \mathbf{c} * \mathbf{a}_l$ for all $j > l$. Hence after a linear transformation of the $\mathbf{a}_1, \ldots, \mathbf{a}_k$ we may assume that $\mathbf{c} * \mathbf{a}_1, \ldots, \mathbf{c} * \mathbf{a}_l$ is a basis of $\mathbf{c} * A$ and $\mathbf{c} * \mathbf{a}_j = 0$ for all $j = l + 1, \ldots, k$. Let D be the subspace of A generated by $\mathbf{a}_{l+1}, \ldots, \mathbf{a}_k$. Then D has dimension $k - l = r$ and $\mathbf{c} * \mathbf{a} = 0$ for all $\mathbf{a}$ in D. So $a_i = 0$ for all $\mathbf{a} \in D$ and $i \in \mathrm{supp}(\mathbf{c})$. Hence

$$\mathrm{supp}(D) \subseteq \{1, \ldots, n\} \setminus \mathrm{supp}(\mathbf{c}).$$

Therefore $d_r(A) \leqslant \mathrm{wt}(D) \leqslant n - \mathrm{wt}(\mathbf{c})$. □

Recall that the *genus* or *Singleton defect* of C is defined by $g(C) = n(C) + 1 - k(C) - d(C)$. This is a nonnegative integer.

Lemma 17.

$$k(\mathbf{c} * A) \geqslant \min\bigl\{\mathrm{wt}(\mathbf{c}) - g(A), k(A)\bigr\}.$$

Proof. Let $l = k(\mathbf{c} * A)$ and $k = k(A)$. Assume that $r = k - l > 0$. Then $d_r(A) \leqslant n - \mathrm{wt}(\mathbf{c})$ by Lemma 16. Now $d_r(A) \geqslant d(A) + r - 1$. Hence

$$d(A) \leqslant n - \mathrm{wt}(\mathbf{c}) - \bigl(k(A) - k(\mathbf{c} * A) - 1\bigr).$$

Or

$$k(\mathbf{c} * A) \geqslant \mathrm{wt}(\mathbf{c}) - g(A). \qquad \square$$

For words $\mathbf{c}$ of sufficiently large weight, at least one of the dimensions $k(\mathbf{c} * A)$ or $k(\mathbf{c} * B)$ is maximal.

Corollary 18. *Let $\mathbf{c} \perp A * B$, and let $\mathrm{wt}(\mathbf{c}) > g(A) + g(B)$. Then*

$$k(\mathbf{c} * A) = k(A), \quad \text{or} \quad k(\mathbf{c} * B) = k(B).$$

Proof. If both $k(\mathbf{c} * A) < k(A)$ and $k(\mathbf{c} * B) < k(B)$, we obtain

$$\mathrm{wt}(\mathbf{c}) \geqslant k(\mathbf{c} * A) + k(\mathbf{c} * B) \geqslant \mathrm{wt}(\mathbf{c}) - g(A) + \mathrm{wt}(\mathbf{c}) - g(B),$$

where the first inequality is implied by Theorem 15 and the second inequality is a consequence of applying Lemma 17 twice. Hence $g(A) + g(B) \geqslant \mathrm{wt}(\mathbf{c})$. This contradicts the assumption. □

Lemma 19. *Let $\mathbf{c} \perp A * B$. Then*

$$\mathrm{wt}(\mathbf{c}) \geqslant \min\bigl\{\mathrm{wt}(\mathbf{c}) - g(A), k(A)\bigr\} + \min\bigl\{\mathrm{wt}(\mathbf{c}) - g(B), k(B)\bigr\}.$$

Proof. Combine Theorem 15 and Lemma 17. □

Theorem 20. [4] *Let $\mathbf{c} \perp A * B$, and let $k(A) > g(B)$ and $k(B) > g(A)$. Then*

$$\mathrm{wt}(\mathbf{c}) \leqslant g(A) + g(B), \quad \text{or} \quad \mathrm{wt}(\mathbf{c}) \geqslant k(A) + k(B).$$

Proof. In the inequality of Lemma 19, four possibilities occur for the right-hand side. Two of these are ruled out by the assumptions. Therefore the two given possibilities remain. □

Remark 21. The Roos-bound for cyclic codes (Theorem 1) is the special case where A, B and C are cyclic, $g(B) = 0$ and $g(A) < k(B)$. Theorem 20 shows that bounds can still be obtained if both A and B have nonzero genus as long as their genus is not too large:

$$g(A) < k(B) \quad \text{and} \quad g(B) < k(A).$$

Theorem 4 uses no condition on $g(B)$ but has a stronger condition on $g(A)$:

$$g(A) < d\big(B^{\perp}\big) - 1.$$

Thus Theorems 4 and 20 are not immediately comparable. There are situations where one does apply and the other does not and vice versa. When

$$g(A) < d\big(B^{\perp}\big) - 1 \quad \text{and} \quad g(B) < k(A)$$

both theorems apply. And in that case $d(C) \geqslant d(B^{\perp}) + k(A) - 1 > g(A) + g(B)$ in Theorem 4 improves to $d(C) \geqslant k(A) + k(B)$ with Theorem 20.

Example 22. [13, Example 3] For cyclic codes, the theorem excludes weights in a way similar to the combination of Theorem 5 and Corollary 1 in [13]. In Example 3 in [13], the code C has zeros at $R \supseteq A'B'$, for

$$A' = \big\{\alpha^i\colon\ 83 \leqslant i \leqslant 95\big\} \cup \big\{\alpha^i\colon\ 98 \leqslant i \leqslant 111\big\},$$
$$B' = \big\{\beta^j\colon\ j = -7, 0, 1\big\}, \quad \beta = \alpha^{16}.$$

With the sets A' and B' we associate codes A and B in the natural way, such that $C \perp (A * B)$. The codes have $k(A) = 27$, $g(A) \leqslant 2$, and $k(B) = 3$, $g(B) \leqslant 6$. The theorem yields: $\mathrm{wt}(\mathbf{c}) \leqslant 2 + 6$, or $\mathrm{wt}(\mathbf{c}) \geqslant 27 + 3$. Clearly $d(C) \geqslant 30$.

Example 23. [6] With the Klein quartic, one can construct codes A, B and C over $GF(8)$ of type $[24, 3, 20]$, $[24, 4, 19]$ and $[24, 16, 7]$, respectively, such that $C \perp (A * B)$. These codes all improve on the Goppa bound by one. It is sufficient to verify this for the two smaller codes A and B. With $k(A) = 3$, $g(A) = 2$, and $k(B) = 4$, $g(B) = 2$, the theorem yields: $\mathrm{wt}(\mathbf{c}) \leqslant 4$, or $\mathrm{wt}(\mathbf{c}) \geqslant 7$. The Goppa bound gives $d(C) \geqslant 6$. So that $d(C) \geqslant 7$.

Theorem 24. *For $0 \leqslant s \leqslant q - 2$, let C be the cyclic code of length $n = q^2 - 1$ over $\mathbb{F}_q$ with defining set $\{i = i_0 + i_1 q\colon\ 0 \leqslant i_0, i_1 \leqslant s\}$. Then C has dimension $k = (q^2 - 1) - (s + 1)^2$. For $2s + 2 \leqslant q + 1$, $d(C) = 2s + 2$. For $2s + 2 \geqslant q$,*

$$d(C) = \begin{cases} [s + 2 - q/2]q, & \text{if } q \text{ is even,} \\ [s + 2 - (q + 1)/2](q + 1), & \text{if } q \text{ is odd.} \end{cases}$$

Proof. Consider first $0 \leqslant 2s + 2 \leqslant q + 1$. The HT bound with $U = \{0, 1, \ldots, s\}$ and $V = \{0, q, \ldots, sq\}$ gives $d \geqslant 2s + 2$. For words with support among the $(q + 1)$th roots of unity the defining set reduces modulo $q + 1$ to the defining set

$$\{-s, -s + 1, \ldots, -1, 0, 1, \ldots, s - 1, s\}.$$

Thus, for $2s+1 < q+1$, the $(q+1)$th roots support an MDS subcode of type $[q+1, q-2s, 2s+2]$. Hence the minimum distance of C is equal to $2s+2$ if $2s+2 \leqslant q+1$.

For $2s+2 \geqslant q$, write $s = t+a$ where a and t are nonnegative integers such that $a \leqslant s+1-q/2$. We obtain a lower bound for the minimum distance by induction on a. Let A and B be codes with generating sets $U = \{0,1,\ldots,t\} + \{0,q,\ldots,aq\}$ and $V = \{0,q,\ldots,tq\} + \{0,1,\ldots,a\}$, respectively. Then $C \perp A * B$,

$$g(A) = g(B) \leqslant g(a) := a(q-t-1) = a(q-s+a-1),$$

and

$$k(A) = k(B) = k(a) := (a+1)(t+1) = (a+1)(s-a+1).$$

Furthermore $g(a) < k(a)$, since $a \leqslant s+1-q/2$. Let $\mathbf{c}$ be a nonzero codeword of C. Then $\mathrm{wt}(\mathbf{c}) \leqslant 2g(a)$ or $\mathrm{wt}(\mathbf{c}) \geqslant 2k(a)$ by the symmetric Roos bound. Now $g(0) = 0$ and $g(a) < k(a-1)$ again since $a \leqslant s+1-q/2$. Hence $\mathrm{wt}(\mathbf{c}) \geqslant 2k(a)$ if $a \leqslant s+1-q/2$, by induction on a. The optimal bound is obtained for $a = \lfloor s+1-q/2 \rfloor$. Hence

$$a+1 = \begin{cases} s+2-q/2, & \text{if } q \text{ is even,} \\ s+2-(q+1)/2, & \text{if } q \text{ is odd,} \end{cases}$$

and

$$t+1 = \begin{cases} q/2, & \text{if } q \text{ is even,} \\ (q+1)/2, & \text{if } q \text{ is odd.} \end{cases}$$

We now construct words of weight equal to the obtained lower bound. A generating set for C is given by

$$I = \{i = i_0 + i_1 q \neq 0 \colon i_0 < q-1-s \text{ or } i_1 < q-1-s\}.$$

When q is even we look for a word of weight $(a+1)q$. In particular, for $s = q-2$ and $a = q/2-1$, we look for a word of weight $q^2/2$. Let $T(x)$ denote the trace function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_2$,

$$T(x) = x + x^2 + \cdots + x^q + x^{2q} + \cdots + x^{q^2/2}.$$

The exponents $i = i_0 + i_1 q$ in $T(x)$ either have $i_0 = 0$ or $i_1 = 0$. Thus the binary word $(\mathrm{Tr}(\alpha^i)\colon\ i = 0,\ldots,q-2)$ belongs to C and has weight $q^2/2$. The nonzero elements are the zeros of

$$T(x) - 1 = \prod_{j=1}^{q/2} \bigl(x + x^q - \alpha_j\bigr),$$

for distinct nonzero elements $\alpha_j \in \mathbb{F}_q$. For $s < q-2$ and $a < q/2-1$, let

$$f(x) = T(x) \cdot \prod_{j=1}^{q/2-1-a} \bigl(x + x^q - \alpha_j\bigr).$$

The exponents $i = i_0 + i_1 q$ in $f(x)$ either have $i_0 < q/2-a$ or $i_1 < q/2-a$. Now $q/2-a = q-1-s$ and thus the word $(f(\alpha^i)\colon\ i = 0,\ldots,q-2)$ belongs to C. It has weight $q^2/2 - (q/2-1-a)q = (a+1)q$. When q is odd we look for a word of weight $(a+1)(q+1)$. In particular, for $s = q-2$ and $a = (q-1)/2-1$, we look for a word of weight $(q^2-1)/2$. Let

$$\tau(x) = x^{t+1} + x^{(t+1)q} = x^{(q+1)/2}\bigl(1 + x^{(q+1)(q-1)/2}\bigr).$$

The exponents $i = i_0 + i_1 q$ in $\tau(x)$ either have $i_0 = 0$ or $i_1 = 0$. Thus the word $(\tau(\alpha^i)$: $i = 0, \ldots, q-2)$ belongs to C and has weight $(q^2-1)/2$. The nonzero elements are the zeros of

$$x^{(q^2-1)/2} - 1 = \prod_{j=1}^{(q-1)/2} \big(x \cdot x^q - \alpha_j\big),$$

for distinct nonzero elements $\alpha_j \in \mathbb{F}_q$. For $s < q-2$ and $a < (q-1)/2 - 1$, let

$$f(x) = \tau(x) \cdot \prod_{j=1}^{(q-1)/2-1-a} \big(x \cdot x^q - \alpha_j\big).$$

The exponents $i = i_0 + i_1 q$ in $f(x)$ either have $i_0 < (q-1)/2 - a$ or $i_1 < (q-1)/2 - a$. Now $(q-1)/2 - a = q - 1 - s$ and thus the word $(f(\alpha^i)$: $i = 0, \ldots, q-2)$ belongs to C. It has weight $(q^2-1)/2 - (q/2 - 1 - a)(q+1) = (a+1)(q+1)$. □

Example 25. The theorem gives as a special case a code C of type $[63, 38, 16]$ over $\mathbb{F}_8$ obtained with $q = 8, m = 2, s = 4$. This is better than the known code $[63, 38, 15]$ that is listed in the Brouwer table [3]. The code C has defining set

$$I = \{0, 1, 2, 3, 4\} + \{0, 8, 16, 24, 32\}.$$

For this particular code, the proof in Theorem 24 comes down to two applications of the AB-method. Let A and B be codes with generating sets U and V, respectively. The choice

$$U = \{0, 1, 2, 3, 4\}, \qquad V = 8 \cdot U$$

corresponds to $g(A) = g(B) = 0$, $k(A) = k(B) = 5$. And thus by Theorem 20, $d(C) \geqslant 10$. The choice

$$U = \{0, 1, 2, 3, 8, 9, 10, 11\}, \qquad V = 8 \cdot U$$

corresponds to $g(A) = g(B) = 4$, $k(A) = k(B) = 8$. And thus by Theorem 20, $d(C) \leqslant 8$ or $d(C) \geqslant 16$. So that $d(C) \geqslant 16$. The same argument applied to the cyclic code of length $n = 65$ defined with

$$I = \{-2, -1, 0, 1, 2\} + \{-16, -8, 0, 8, 16\}$$

gives a code of type $[65, 40, 16]$ that is better than the known code $[65, 40, 15]$ that is listed in the Brouwer table [3].

References

[1] R.C. Bose, D.K. Ray-Chaudhuri, On a class of error-correcting binary group codes, Inform. Control 3 (March 1960) 68–79.

[2] R.C. Bose, D.K. Ray-Chaudhuri, Further results on error-correcting binary group codes, Inform. Control 3 (September 1960) 279–290.

[3] A.E. Brouwer, Bounds on the minimum distance of linear codes, http://homepages.cwi.nl/htbin/aeb/lincodbd.

[4] I.M. Duursma, Decoding linear codes, preprint CNRS UPR-9016, Luminy, France, 1994.

[5] I.M. Duursma, R. Kötter, Error-locating pairs for cyclic codes, IEEE Trans. Inform. Theory IT-40 (1994) 1108–1121.

[6] I.M. Duursma, Monomial embeddings of the Klein curve, in: G. Faina (Guest-Ed.), Discrete Math. 208/209 (1999) 235–246.

[7] G.-L. Feng, K.K. Tzeng, A generalization of the Berlekamp–Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes, IEEE Trans. Inform. Theory IT-37 (September 1991) 1274–1287.
[8] G.-L. Feng, K.K. Tzeng, Decoding cyclic and BCH codes up to actual minimum distance using nonrecurrent syndrome dependence relations, IEEE Trans. Inform. Theory IT-37 (November 1991) 1716–1723.
[9] G.-L. Feng, K.K. Tzeng, A new procedure for decoding cyclic and BCH codes up to actual minimum distance, IEEE Trans. Inform. Theory IT-40 (September 1994) 1364–1374.
[10] C.R.P. Hartmann, K.K. Tzeng, Generalizations on the BCH bound, Inform. Control 20 (1972) 489–498.
[11] A. Hocquenghem, Codes correcteurs d'erreurs, Chiffres 2 (September 1959) 147–156.
[12] R. Kötter, An unified description of an error locating procedure for linear codes, in: Proc. Int. Workshop Algebraic Combinator. Coding Theory, Voneshta Voda, Bulgaria, 1992.
[13] J.H. van Lint, R.M. Wilson, On the minimum distance of cyclic codes, IEEE Trans. Inform. Theory IT-32 (1986) 23–40.
[14] R. Pellikaan, On decoding linear codes by error correcting pairs, preprint, Eindhoven University of Technol., 1988.
[15] R. Pellikaan, On decoding by error location and dependent sets of error positions, Discrete Math. 106–107 (1992) 369–381.
[16] R. Pellikaan, On the existence of error-correcting pairs, J. Statist. Plann. Inference 51 (1996) 229–242.
[17] R. Pellikaan, The shift bound for cyclic, Reed–Muller and geometric Goppa codes, in: R. Pellikaan, M. Perret, S.G. Vlăduţ (Eds.), Arithmetic, Geometry and Coding Theory 4, Luminy, 1993, de Gruyter, Berlin, 1996, pp. 155–174.
[18] C. Roos, A generalization of the BCH bound for cyclic codes, including the Hartmann–Tzeng bound, J. Combin. Theory Ser. A 33 (1982) 229–232.
[19] C. Roos, A new lower bound for the minimum distance of a cyclic code, IEEE Trans. Inform. Theory IT-29 (1983) 330–332.
[20] B.-Z. Shen, K.K. Tzeng, A code decomposition approach for decoding cyclic and algebraic–geometric codes, IEEE Trans. Inform. Theory 41 (November 1995) 1969–1987.
[21] K.K. Shen, C. Wang, K.K. Tzeng, B.-Z. Shen, Generation of matrices for determining minimum distance and decoding of cyclic codes, IEEE Trans. Inform. Theory 42 (March 1996) 653–657.